



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/576,412	05/22/2000	Gilles Lisimaque	032326-025	1838
21839	7590	06/16/2004	EXAMINER	
BURNS DOANE SWECKER & MATHIS L L P			WU, ALLEN S	
POST OFFICE BOX 1404			ART UNIT	
ALEXANDRIA, VA 22313-1404			PAPER NUMBER	

2135

DATE MAILED: 06/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/576,412

Applicant(s)

LISIMAQUE, GILLES

Examiner

Allen S. Wu

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 April 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 May 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ieki et al (hereinafter Ieki), US Patent 5,204,512, in view of Chen et al (hereinafter Chen), US Patent 5,694,471, and further in view of Bosen et al, US Patent 5,060,263.

As per claim 1, Ieki discloses a means of managing data stored in a first memory of a first chip card of a first chip card (see abstract) in which:

a first management code is recorded in the first memory (see for example; col 3 ln 58-col 4 ln 4), the first card is linked to a chip card reader (see for example; card detectors, col 3 ln 25-31 and fig 1), and

editing of data stored in the first memory is authorized if a secret code (code number or password) presented to the reader is compatible with the recorded first management code (see for example; col 3 ln 64-col 4 ln 4),

wherein the following steps are performed:

data relating to the first card and the second management code are recorded in a second memory of a second chip of the second chip card (see for example; col 4 ln 38-46 and col 4 ln 62-67), and

editing of the data stored in the second memory is authorized if a secret code (code number or password) presented to the reader is compatible with the recorded second management code (see for example; col 4 ln 32-46).

Ieki does not explicitly teach a first management code produced with a first cryptographic algorithm based on a mother key and a first set of identification data of the first chip card. Chen further discloses a method of access protection on a chip card including producing a management code (PIN) with a first cryptographic algorithm (encryption) and a set of identification data of the first chip card (see for example; col 8 ln 46-59). Chen further discloses the means of such generation of management codes provide a means of higher security and authenticity of the cards (see for example; col 3 ln 26-41). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to use the management code generation of Chen within the system of Ieki to generate the management code because it would have provided a secure means of generating a management code that is high in authenticity in the system of Ieki.

Ieki-Chen discloses the means of generating a management codes for a chip card based on identification data of the chip card and authorizing editing of data stored in the memory of the chip card, as described above. Ieki-Chen does not explicitly teach generation of a second management code with a second cryptographic algorithm based on data relating to the first card and a second set of identification data of a second chip card. Bosen discloses a access control

system comprising of dynamic management codes (see for example; col 4 ln 15-49) wherein the second management code is generated based on prior data and new data (see for example; col 4 ln 27-49 col 6 ln 58-67) and that such generation can be carried out by a chip card (see for example; portable password issuing devices, col 4 ln 50-62). Bosen further discloses use of dynamic passwords being well known in the art to promote security since passwords are generated dynamically and are linked to each other (see for example; col 4 ln 27-49). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Bosen within the Ieki-Chen combination because it would have provided a means of generating a second management code, which is linked with a first management code. In smart card replacements, linking of the second card with a first card is well known in the art and further provides an extra layer of authenticity of the replacement card.

As per claims 2, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Ieki further discloses the first and second management codes are secret codes (see for example; col 3 ln 64-67 and col 4 ln 38-46; Such use of code number implies that the first and second management codes must be secret codes to keep the integrity and purpose of the codes for authorization requests).

As per claim 3, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Chen further discloses that the cryptographic algorithms are performed in the chip of the card (see for example; col 8 ln 46-59) and is rejected under the same rationale of producing management codes described above (see claim 1).

As per claim 4, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Ieki discloses a first cryptographic algorithm for communication being different from a second cryptographic algorithm (see for example; col 2 ln 12-24). Switching cryptographic algorithms are well known in the art to increase security by eliminating attacks by trial and error and reverse engineering. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to incorporate such switching of algorithms because it would have provided an increase in code integrity by avoiding such attacks. Bosen further discloses the second cryptographic algorithm is symmetric (see for example; DES, col 4 ln 63-65). Such algorithms are rejected under the same rationale of dynamic passwords as described above (see claim 1).

As per claim 5, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Bosen further discloses that the first cryptographic algorithm is the same as the second cryptographic algorithm (see

for example; DES, col 4 ln 63-65). Such algorithms are rejected under the same rationale of dynamic passwords as described above (see claim 1).

As per claim 6, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Chen further discloses generating management codes using data relating to a first card and that the use of such a generating means increases protection of forgery and duplication of an existing card by copying. One of ordinary skill in the art at the time of the applicant's invention would have realized that in such a combination, generation of passwords are based on identification. It would have been obvious for such generation of passwords in the Ieki-Chen-Bosen combination because it would have provided additional protection of card fraud and copying.

As per claim 7, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). As per the data relating to the first card is the first management code of the first card or the first chip card, Bosen further discloses the prior data being a first management code (see for example; col 4 ln 27-32). Such data for generating a second management code is rejected under the same rationale of management code generating described above (see claim 1).

As per claim 8, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Ieki does not explicitly teach a determination of

whether the card is authentic. Chen further discloses a determination being made of whether the card is authentic if said management code word produced in the reader on the basis of the data relating to the first card is compatible with a second key word (see for example; digital signature, col 9 ln 56-col 10 ln 11), and that such determination of authenticity prevents cards from being duplicated by copying (see for example; col 3 ln 26-41). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the determination means of Chen within the system of Ieki because it would have increased security and authenticity by preventing card forgery and copying.

3. Claims 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ieki et al (hereinafter Ieki), US Patent 5,204,512, in view of Chen et al (hereinafter Chen), US Patent 5,694,471, and further in view of Bosen et al, US Patent 5,060,263, and further in view of Drupsteen et al, US Patent 6,073,238.

As per claim 9, Ieki-Chen-Bosen discloses the claimed limitations as described above (see claim 1). Ieki-Chen-Bosen does not disclose a transmission attribute associated with the data stored in the first memory. Drupsteen discloses storing the data with a transmission attribute (flag register, col 4 ln 17-39), the use of attributes to specify commands to be processed (col 5 ln 17-39), and copying of the attribute into a memory (flag register associated with master file, fig 4, col 5 ln 17-39). As for the attribute giving information about a need to produce a second secret code when copying data, Drupsteen further

discloses the use of attributes to specify commands to be processed (col 5 ln 17-39). One of ordinary skill in the art at the time of the applicant's invention would have modified the Ieki-Chen-Bosen combination to further associate a transmission attribute with data stored in the first memory. Both the Ieki-Chen-Bosen combination and Drupsteen discloses a method of managing data in a chip card and transmission of data from a card. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Drupsteen within the Ieki-Chen-Bosen combination because it would have added flexibility to the chip card. The addition of attributes can allow the chip card to perform certain commands depending on the attribute.

As per claim 10, Ieki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 9). Ieki further discloses editing of data under the control of a master system (see for example; col 4 ln 47-63). Ieki-Chen-Bosen does not explicitly teach reading an attribute prior to editing and an editing program is started if the attribute having been read allows this. Drupsteen discloses reading the attributes before processing a command (col 5 ln 17-28) and use of attributes to inhibit or allow certain commands to be processed (col 5 ln 17-35). One of ordinary skill in the art at the time of the applicant's invention would have modified the combination of Ieki-Chen-Bosen so that an attribute is read before data on the card is edited. It would have been obvious to one of

ordinary skill in the art at the time of the applicant's invention to combine the teachings of Drupsteen within the Ieki-Chen-Bosen because it would have heightened security. Reading an attribute before processing a command or program allows the combination to inhibit editing depending on the attribute. Furthermore, using the attributes inhibits the execution of a command. Therefore, unwanted commands or programs will not start if the attribute is set to a certain value.

As per claim 11, Ieki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 9). Ieki-Chen-Bosen does not teach the transmission attribute inhibiting editing. Drupsteen further discloses the use of attributes to inhibit or allow certain commands to be processed (col 5 ln 17-35). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Drupsteen within the Ieki-Chen-Bosen combination because it would have heightened security. Using attributes allows the system to inhibit the execution of a command. Therefore, unwanted commands or programs will not start if the attribute is set to a certain value.

As per claim 12, Ieki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 9). Ieki further discloses data copied into the memory in delayed time (see for example; fig 1 and col 4 ln 63-67; the

data being written into the card is enciphered first by a host, thus creating a delay before it is copied).

As per claim 13, Ieki-Chen-Bosen-Drupsteen discloses the claimed limitations as described above (see claim 1). Chen further discloses the card being a multi-application card (see for example; col 3 ln 41-51). Ieki-Chen-Bosen does not explicitly teach data being associated with respective management codes. Drupsteen discloses respective management codes for each application (K3*, col 5 ln 1-16). Chip cards contain processors, which can be programmed for different tasks. One of ordinary skill in the art at the time of the applicant's invention would have modified the combination of Ieki-Chen-Bosen so as to incorporate different management codes for each application. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the respective management codes of Drupsteen within the Ieki-Chen-Bosen combination because it would have heightened security. The use of respective management codes will insure that one the data pertaining to certain applications are processed.

Response to Arguments

4. The Information Disclosure Statement filed May 22, 2000 has been fully considered. A copy is attached.

5. Applicant's arguments, see page 7, filed 2 April 2004, with respect to claims 8-11 and 13 have been fully considered and are persuasive. The rejection under 35 USC 112 of claims 8-11 and 13 has been withdrawn.

6. Applicant's arguments, see pages 8-10, filed 2 April 2004, with respect to the rejection(s) of claim(s) 1-13 under 35 USC 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newly found prior art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/576,412
Art Unit: 2135

Page 12

Allen Wu
Patent Examiner
Art Unit 2135

ASW


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100